

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
Alexandria Division

UNITED STATES OF AMERICA,	)	
	)	
Plaintiff,	)	
v.	)	Civil Case No. 1:25-cv-555
	)	
330,000.026094 USDT TOKENS SEIZED FROM THE	)	
CRYPTOCURRENCY WALLET ADDRESS	)	
IDENTIFIED BY	)	
0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1	)	
	)	
Defendant <i>in Rem</i> .	)	

**COMPLAINT FOR FORFEITURE IN REM**

COMES NOW the plaintiff, United States of America, by and through its counsel, Erik S. Siebert, United States Attorney for the Eastern District of Virginia and by Annie Zanobini, Assistant United States Attorney, brings this complaint and alleges as follows in accordance with Supplemental Rule G(2) of the Federal Rules of Civil Procedure:

**NATURE OF THE ACTION**

1. The United States brings this action *in rem* seeking the forfeiture of all right, title and interest in the 330,000.026094 USDT Tokens seized from the cryptocurrency wallet address identified by 0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1 (“Defendant Property”), involving violations of 1956(a)(1)(B)(i) (concealment money laundering). The Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

### **THE DEFENDANT IN REM**

2. Defendant 330,000.026094 USDT tokens were seized from a cryptocurrency wallet address identified by 0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1 and is currently held in a cryptocurrency wallet address controlled by the Federal Bureau of Investigation (“FBI”) in the Eastern District of Virginia.

### **JURISDICTION AND VENUE**

3. This Court has subject matter jurisdiction over an action commenced by the United States under 28 U.S.C. § 1345, and over an action for forfeiture under 28 U.S.C. § 1355(a) and (b).

4. This Court has *in rem* jurisdiction over the Defendant Property under 28 U.S.C. § 1355(b)(1)(B) with reference to 18 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

5. Venue is proper in this judicial district under 28 U.S.C. § 1355(b)(1)(B) with reference to 18 U.S.C. § 1395(b) because the Defendant Property is located in the Eastern District of Virginia and under 28 U.S.C. § 1355(b)(1)(A) because acts and omissions giving rise to the forfeiture took place in the Eastern District of Virginia.

### **BASIS FOR FORFEITURE**

6. 18 U.S.C. § 981(a)(1)(A) provides for the forfeiture of any property, real or personal, involved in a violation or attempted violation of 18 U.S.C. § 1956, or any property traceable to such property.

## STATEMENT OF FACTS

7. The FBI seized the Defendant Property from criminals involved in investment fraud scams. The United States of America seeks to lawfully forfeit the Defendant Property to punish and deter criminal activity by depriving criminals of property used in or acquired through illegal activities and to recover assets that may be used to compensate victims.<sup>1</sup>

A. Background on cryptocurrency

8. **Virtual Currency:** Virtual currencies are digital tokens of value circulated over the Internet as substitutes for traditional fiat currency. Virtual currencies are not issued by any government or bank like traditional fiat currencies such as the U.S. dollar, but rather are generated and controlled through computer software. Bitcoin is currently one of the most popular virtual currencies in use.

9. **Virtual Currency Address:** Virtual currency addresses are the digital locations to which such currencies are sent and received. A virtual currency address is analogous to a bank account number and is represented as a string of letters and numbers. It is possible to “swap” or otherwise exchange cryptocurrencies by using Decentralized Exchanges (DEXs). DEXs allow for the swapping of one cryptocurrency for another by keeping large liquidity pools of various cryptocurrency types, which users can then swap between for a nominal fee. Unlike Centralized Cryptocurrency Exchanges, DEXs are not custodial, and allow for these swaps through the use of smart contracts, and therefore avoid the need for a third party to ever have custody of the cryptocurrencies being swapped. A DEX does not collect Know Your Customer (KYC) information.

---

<sup>1</sup> See United States Asset Forfeiture Program, *Our Mission*, <https://www.justice.gov/afp>.

10. **Virtual Currency Exchange:** Virtual currency exchanges, such as Crypto.com, are trading and/or storage platforms for virtual currencies. Many exchanges also store their customers' virtual currency in virtual currency accounts. These virtual currency accounts are commonly referred to as wallets and can hold multiple virtual currency addresses.

11. **Blockchain:** Many virtual currencies, including Ether, publicly record all their transactions on what is known as a blockchain. The blockchain is a distributed public ledger containing an immutable and historical record of every transaction utilizing that blockchain's technology. The blockchain can be updated multiple times per hour and records every virtual currency address that has ever received that virtual currency and maintains records of every transaction and all the known balances for each virtual currency address. There are different blockchains for different types of virtual currencies. Due to the international nature of virtual currencies, most blockchain explorers operate using the Coordinated Universal Time (UTC) Zone. The times/dates used in this complaint are also based on the UTC time zone.

12. **Blockchain Analysis:** While the identity of a virtual currency address owner is generally anonymous, law enforcement can identify the owner of a particular virtual currency address by analyzing the blockchain. The analysis can also reveal additional addresses controlled by the same individual or entity.

13. **Stablecoins:** Stablecoins are a type of virtual currency whose value is pegged to a commodity's price, such as gold, or to a fiat currency, such as the U.S. dollar, or to a different virtual currency. For example, Tether (USDT) is a stablecoin pegged to the U.S. dollar. Stablecoins achieve their price stability via collateralization (backing) or through algorithmic mechanisms of buying and selling the reference asset or its derivatives.

14. **Tether (USDT):** Tether Limited (“Tether”) is a company that manages the smart contracts and the treasury (i.e., the funds held in reserve) for USDT tokens.

15. **Ether:** Ether (“ETH”) is a cryptocurrency that is open-source and is distributed on a platform that uses “smart contract” technology. Transactions involving ETH are publicly recorded on the Ethereum blockchain, which allows anyone to track the movement of ETH.

16. **Bitcoin:** Bitcoin (or “BTC”) is a type of virtual currency. Unlike traditional, government-controlled currencies (i.e., fiat currencies), such as the U.S. dollar, Bitcoin is not managed or distributed by a centralized bank or entity. Because of that, Bitcoin can be traded without the need for intermediaries. Bitcoin transactions are approved/verified by computers running Bitcoin’s software. Those computers are called network nodes. Each node uses cryptography to record every Bitcoin transaction on the Bitcoin blockchain. The Bitcoin blockchain is a public, distributed ledger. Bitcoin can be exchanged for fiat currency, other virtual currencies, products, and services.

B. The Investment Fraud Scheme

17. This complaint involves criminal syndicates operating cryptocurrency investment fraud schemes. The scammers promoted spoofed domains and websites purporting to look like legitimate cryptocurrency trading platforms to U.S. victims. Scammers then fooled victims into “investing” in cryptocurrency through these fraudulent investment platforms, which instead allowed the scammers to steal their money.

18. This type of scam involves scammers spending significant time getting to know and grooming their victims to gain their confidence. After developing a relationship and gaining trust, scammers instruct their victims to visit the spoofed domains to get them to make significant

capital investments in what victims believe are legitimate cryptocurrency trading platforms. The victims are then typically asked to invest their funds via wire transfer or through a provided cryptocurrency deposit address. While the scammers prefer cryptocurrency deposits, they will also accept bank wires if the victim cannot transfer cryptocurrency.

19. As part of the scheme to defraud, the victims are told that they can expect to make a sizeable return on their investments. As investments are made, the spoofed websites falsely displayed a significant increase in the victim's account balance, which encouraged the victim to continue making investments. When the victim attempted to make a withdrawal, the scammers often attempted to coerce the victims to send even more funds. These tactics included requesting additional deposits due to "significant profits" gained on the account or other reasons such as freezing the account due to "taxes owed" or "suspicious behavior." Regardless of how the scammers attempted to solicit additional investments from the victims, the victims were unable to recover their investment.

20. The criminals then move the victim funds beyond reach of law enforcement, typically by using non-custodial or "private" wallets that law enforcement cannot attribute using legal process or blockchain analysis alone; by transferring victim funds through multiple wallets before those funds reach a consolidation wallet; and by commingling victim funds with other funds in a consolidation wallet and sometimes then further transferring the funds to additional "downstream" wallets. Criminals frequently liquidate their cryptocurrency fraud proceeds by using "brokers" who agree to buy the cryptocurrency in exchange for other currency, including fiat currency.

C. The Scheme and VICTIM 1

21. On or about July 15, 2024, the victim, a resident of Arlington, Virginia, which is in the Eastern District of Virginia, contacted the Federal Bureau of Investigation to report that they were the victim of fraud. The victim reported that they were defrauded out of approximately \$86,158.00.

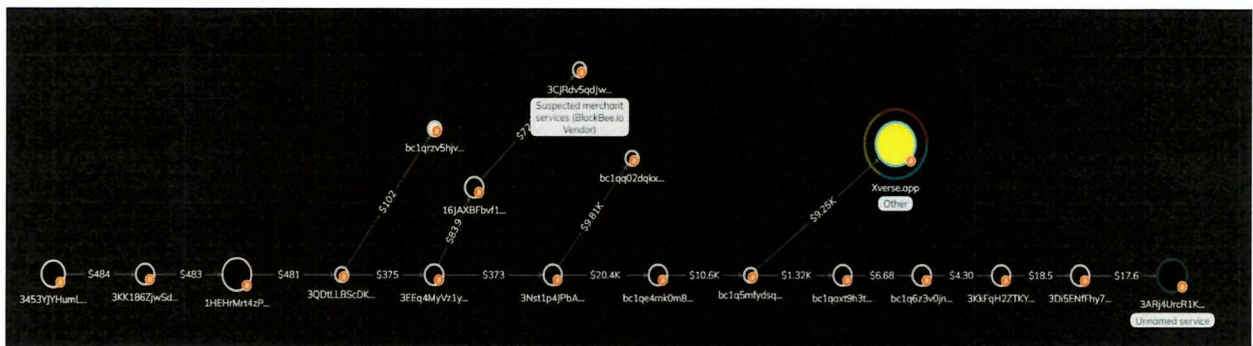
22. In June of 2024, the victim met the unknown subject(s), purportedly a man named “David” via Bumble, an online dating application. After matching on Bumble and speaking through Bumble’s chat function, David suggested that they chat on Whatsapp. During their conversation via Whatsapp, David claimed to be knowledgeable about short-term cryptocurrency trading, and eventually convinced the victim to begin investing with David’s assistance.

23. David walked the victim through setting up an account at Crypto.com, which is a Cryptocurrency exchange. David explained that the victim could use the Crypto.com account to purchase cryptocurrency and then move that cryptocurrency into a Decentralized Finance (DeFi) wallet app. Once in the Defi wallet app, the victim was informed they could invest the cryptocurrency in a trading platform called Trustfuturesnum.com (“Trustfutures”). The investigation revealed that Trustfuturesnum.com was created on or about February 2, 2024.

24. DeFi wallet apps are virtual asset wallet applications in which users can participate in the finance sector without the use of traditional intermediaries such as brokerages, banks, or exchanges. Instead, the users can participate in investing, lending, borrowing, or other similar actions through peer-to-peer transactions, thus decentralizing the financial transactions from traditional intermediaries.



25. In June of 2024, at the direction of David, the victim made an investment account at Trustfutures. On or about June 17, 2024, the victim sent \$500.00 from their CashApp account to their Crypto.com account. The victim then used their Crypto.com account to purchase 0.0073119 Bitcoin (BTC), valued at approximately \$483.00 USD. The victim then sent the 0.0073119 BTC to what the victim believed was their Trustfutures account. However, in actuality, the victim sent the BTC to an unhosted BTC address, 1HEHrMrt4zPPFoggkUKYdnKSPADgCWMHW3, which is unrelated to any legitimate trading platform. This BTC was then sent by the subject(s) with control of this wallet to other wallets which eventually depleted the funds. A visual representation of the movement of the BTC is below:



26. Following this initial investment, the victim's Trustfutures account appeared to show significant returns on the victim's initial investment. After seeing what the victim believed to be the initial returns, the victim made additional investments. Over the course of the following few weeks, the victim conducted four more investment transactions totaling \$83,436.16. Following these transactions, the victim believed they had made significant profit as their Trustfutures account showed a balance of \$322,803.99.



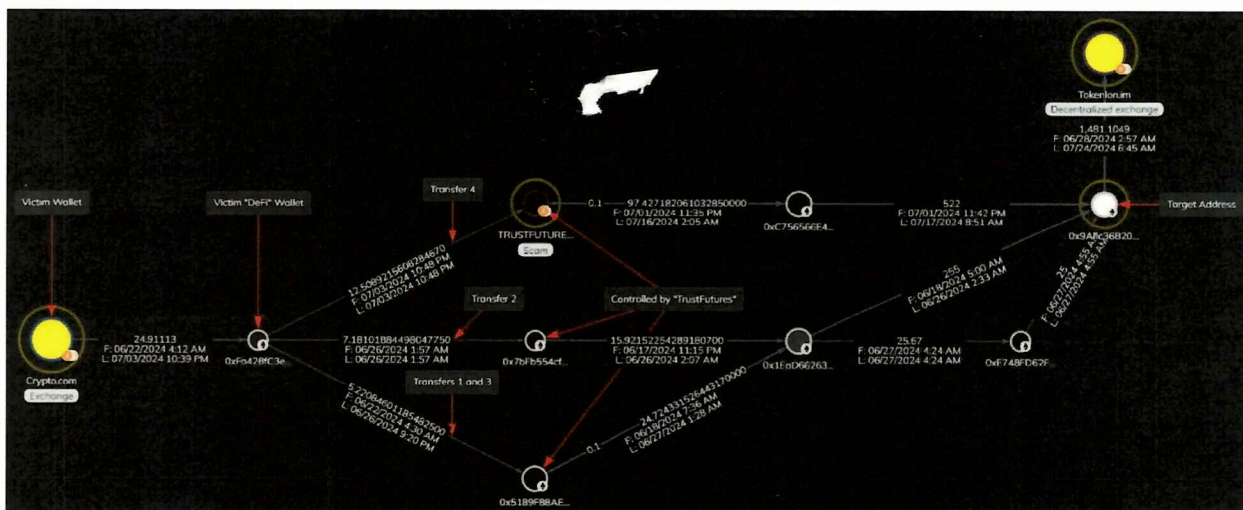
27. On or about July 9, 2024, the victim attempted to withdraw funds from their Trustfutures account. However, upon attempting to withdraw funds, David became combative with the victim and refused to approve the withdrawal. The victim used the chatbot function on Trustfutures to contact customer service about the withdrawal. Trustfutures Customer Service told the victim that in order to make a withdrawal the victim would first need to pay a 15% withdrawal fee in the amount of approximately \$48,420.45. The victim was further told that if this fee was not paid within 7 business days, the funds might be lost in the blockchain.

28. The victim contacted David again and requested that David provide screenshots of his transactions from his Trustfutures account to prove that if an account holder pays the withdrawal fee, then the company will release the funds. David provided the victim with some screenshots; however, the victim noticed several typos including the spelling of David's name. The inability of the victim to make a withdrawal, the tactic of asking for additional fees, and the screenshots containing typos caused the victim to suspect that Trustfutures was an investment scam.

29. On or about July 15, 2024, the victim submitted a complaint to the FBI and was interviewed by the FBI on or about July 18, 2024.

30. Law enforcement traced each of the subsequent four transactions and the tracing shows that the cryptocurrency was not placed in the victim's investment account at Trustfutures. Instead, it was laundered through multiple Ethereum addresses before being deposited in 0x9AFc36B20C961CD34450ae0C3941C302bfd6B1F1 (0x9AF). The four transactions from the victim totaled approximately 24.9 Ethereum. Below is a visual representation of the movement of the four transactions and the interconnectivity of many of these wallet addresses. It should be

noted that the values of transferred ETH shown on the visual representation are the values of the total amount of ETH transferred between two clusters between the dates that are listed. They do not necessarily represent single transfers of ETH.



### ***Transaction 1 – June 22, 2024, 04:12 UTC***

31. On June 22, 2024, the victim transferred approximately 1.67253 ETH (valued at approximately \$5,861.70) from their Crypto.com account to their DeFi wallet, which the victim had also created with the assistance of David. About 18 minutes later, the victim transferred approximately 1.67247 ETH from their DeFi wallet to 0x5189F88AEf4412120Db1Bad65329A55B4a08f2Fa (0x51), an address controlled by the individual(s) behind the scam.

32. About 7 minutes later, approximately 1.67241 ETH was transferred from 0x51 to 0x1EaD66263c6559fc5868Ec7C2d7714CCcdCe4Bf9 (0x1EaD), where it was comingled with other funds. It remained in this address for about 5 days.

33. On June 27, 2024, 0x1EaD transferred approximately 25.67 ETH, including the victim funds, to 0xE748FD62F1671a1bc37A6e41FD16B1DcAA5Df357 (0xE7). About 31 minutes later, 0xE7 transferred approximately 25.00 ETH to 0x9AF.

***Transaction 2 – June 26, 2024, 01:43 UTC***

34. On June 26, 2024, the victim transferred approximately 7.18109 ETH (valued at approximately \$24,328.88) from their Crypto.com account to their DeFi wallet. About 14 minutes later, the victim transferred approximately 7.18101 ETH from their DeFi wallet to 0x7bFb554cf05430FA19F1F75A0f03AAa535f811bb (0x7b), an address controlled by the individual(s) behind the scam.

35. About 10 minutes later, approximately 7.18095 ETH was transferred from 0x7b to 0x1EaD, where it was comingled with other funds.

36. About 26 minutes later, 0x1EaD transferred approximately 28.00 ETH, including the victim funds, to 0x9AF.

***Transaction 3 – June 26, 2024, 21:12 UTC***

37. About 19 hours and 29 minutes after the previous transaction conducted on June 26, 2024, the victim transferred approximately 3.5485 ETH (valued at approximately \$12,027.07) from their Crypto.com account to their DeFi wallet. About 8 minutes later, the victim transferred approximately 3.54837 ETH from their DeFi wallet to 0x5189F88AEf4412120Db1Bad65329A55B4a08f2Fa (0x51), an address controlled by the individual(s) behind the scam.

38. About 29 minutes later 3.5483 ETH was transferred from 0x51a to 0x1EaD, where it was comingled with other funds. It remained in this address for about 6 hours and 35 minutes.

39. On June 27, 2024, 0x1EaD transferred approximately 25.67 ETH, including the victim funds, to 0xE748FD62F1671a1bc37A6e41FD16B1DcAA5Df357 (0xE7). About 31 minutes later, 0xE7 transferred approximately 25.00 ETH to 0x9AF.

***Transaction 4 – July 3, 2024, 22:39 UTC***

40. On July 3, 2024, the victim transferred approximately 12.50901 ETH (valued at approximately \$41,218.51) from their Crypto.com account to their DeFi wallet. About 14 minutes later, the victim transferred approximately 12.50892 ETH from their DeFi wallet to 0xd19632f884fE059C0Ed20f23912224015080C094 (0xd1), an address controlled by the individual(s) behind the scam. It should be noted that due to previous activity in this address, blockchain analysis had already identified 0xd1 as being involved in a scam associated with TRUSTFUTURESCY.com. In the visual below paragraph 30, the cluster bubble appears with a yellow circle and the word “SCAM” directly under it.

41. About 5 minutes later approximately 12.50892 ETH was transferred from 0xd1 to 0xC756566E4ad94764F1F00aBc4b650060Af99F891 (0xC756), where it was comingled with other funds.

42. The following day, on July 4, 2024, 0xd1 transferred approximately 35.00 ETH, including the victim funds, to 0x9AF.

***Activity of 0x9AF and Movement of Funds***

43. 0x9AF was created first on June 18, 2024, and continued to be active through at least August 2, 2024.

44. Over the course of this timespan, 0x9AF received approximately 1672.77 ETH, which is roughly equivalent to \$5,309,927.86 USD. Of that, at least 457.97 ETH of the ETH that 0x9AF received was done, either directly or indirectly, from other Ethereum addresses which are associated with previously identified investment scams. Of note, in addition to indirectly receiving funds from 0xd1, which is identified as being connected to “TRUSTFUTURESCY.com” (previously described above), 0x9AF also received indirect funding from other, similarly named scam clusters. Examples of such clusters are 0x2B99e2D6a4DA4F8231eBd566B571c4E71fb61eD5, identified as “TRUSTFUTURESBIT.com”, 0x2B99e2D6a4DA4F8231eBd566B571c4E71fb61eD5, identified as “TRUSTFUTURESOPT.com”, and other similar names, often including the words “Trust”, “DeFi”, and/or “Futures”. These names indicate, falsely, that they are related to futures trading and/or investing.

45. More specifically, two consolidation addresses previously mentioned, 0xC756 and 0x1EaD, received a significant amount of ETH from clusters tied to other, similar investment fraud schemes.

46. 0xC7 was active between July 1, 2024, and July 17, 2024. During this timeframe, it received approximately 545.63 ETH. Of this, approximately 325.9115 ETH came directly from 8 other clusters connected to related investment fraud schemes.

47. 0x1EaD was active between June 17, 2024 and June 27, 2024. During this timeframe, it received approximately 285 ETH. Of this, approximately 41.86 ETH came directly from 4 other clusters connected to related investment fraud schemes.

48. Furthermore, for both 0xC756 and 0x1EaD, their remaining funding originated almost exclusively from Crypto.com, and entered 0xC756 and 0x1EaD from intermediary wallets. It is common for those perpetrating this type of investment fraud scheme to direct many of their victims to open accounts using the same Cryptocurrency Exchanges. In this particular scheme, the victim was directed to open an account using Crypto.com.

49. While 0x9AF received ETH directly and indirectly from multiple different sources, 0x9AF sent ETH almost exclusively to one location, Tokenlon. Of the approximately 1,581.2149 ETH that 0x9AF sent, approximately 1481.1049 ETH (about 93.66%) to Tokenlon. Tokenlon is DEX.

50. Those perpetrating the type of investment fraud scheme described in this complaint often use DEXs or similar swapping services to further their schemes. Using a DEX and swapping one virtual asset for another further obfuscates the origin of the virtual assets and causes the tracing of such virtual assets to become more complex.

51. It is also common to use DEXs to swap native tokens, such as Ether, to Stablecoins. Victims are commonly told to invest using virtual assets such as Bitcoin or Ether. While the victims are interested in investing with tokens that are subject to market changes, the scammers typically are not. To protect the value of the funds fraudulently obtained, scammers will often use DEXs or other swapping services to swap more volatile virtual assets to stable

ones, particularly stablecoins pegged to the US Dollar, which as a fiat currency, is generally stable and strong in comparison to many other types of fiat foreign currencies.

52. Of the approximately 1672.77 ETH that 0x9AF has received, 0x9AF has sent approximately 1481.2149 ETH to Tokenlon, where the ETH was swapped for Tether (USDT) and returned to 0x9AF.

53. Once swapped, 0x9AF would then withdraw the USDT and send it to other addresses to continue the movement and concealment of the funds. The USDT would then eventually be sent to Exchange accounts held in exchanges that are based overseas and outside the jurisdiction of the United States. These series of convoluted transactions and quick swaps from one type of cryptocurrency to another is a strong indication that the movement of funds was performed in a manner meant to conceal the nature, source, control, and/or ownership of the proceeds of a specified unlawful activity. With respect to the scheme alleged in this complaint, the specified unlawful activity is wire fraud, in violation of 18 U.S.C. § 1343.

54. 0x9AF was held in an unhosted wallet that had the capability of generating and using addresses that operate on the Ethereum Blockchain. This allowed 0x9AF to send and receive both ETH and USDT by using the same Ethereum address.

55. Since Transaction 1 reached 0x9AF on June 27, 2024, through July 30, 2024, 0x9AF has carried a large balance of ETH. Since the first transaction into 0x9AF containing funds obtained fraudulently from the victim, 0x9AF has never held less than 141.6552 ETH (valued at approximately \$425,904.77) at any given time. As the amount of ETH in 0x9AF has never dropped below 24.9 between the day the victim's funds entered 0x9AF and the date 0x9AF was frozen, as described below, the victim's funds remain in the account as ETH.



56. As all the funds currently held in 0x9AF are involved in money laundering, all of the funds—both ETH and USDT—are subject to forfeiture. While the victim transfers may have entered 0x9AF as ETH, any USDT located within 0x9AF constitutes property involved in money laundering as it helped conceal the nature, source, location, control, and/or ownership of the proceeds of a specified unlawful activity, to wit, wire fraud.

57. On July 30, 2024, Tether implemented a voluntary freeze of 0x9AF and informed FBI that the balance in the address was 300,000 USDT.

58. The 300,000 USDT initially came from Sideshift.ai, an exchange and swapping service which is located in St. Kitts and Nevis. From Sideshift, the funds were sent as ETH into two unhosted addresses, 0xA85975b9E69b589780A6a38b3A0128C5cE379d04 and 0xA525fa18D6b04538618B6a1AA8AC68c71eD262c0. Those addresses, in turn, sent the funds to a consolidation address, 0x6687F0e00B6C618e3A48045B253b08f5173684b7, which swapped the ETH for USDT via Tokenlon. Following this, the funds were sent to 0x0D3B28EFF27670a3ADE8179cBB72F5efa63D672F (0x0D3), which then sent them to 0x9AF, where they were frozen.

59. In addition to this 300,000 USDT specifically, between July 23, 2024 and July 30, 2024, 0x0D3 transferred an additional 680,000 USDT to 0x9AF. 0x0D3, in total, sent approximately 980,000 USDT to 0x9AF across four separate transactions within about seven days.

60. The pattern of movement for these funds is consistent with the movement of funds previously described with the victim's funds and with other cryptocurrency sent to 0x9AF from other, related, scam addresses. In all of these situations, ETH was transferred in an

impractical manner through multiple unhosted wallets. This movement incurred an excessive amount of gas fees, which investors generally try to minimize. Then, in all of these situations, Tokenlon was used to swap ETH to USDT. As previously described, this is a very common methodology employed by scammers in these types of investment fraud scams. This allows scammers both to obfuscate the nature and origin of these funds, while simultaneously protecting the value of their assets by moving away from a more volatile virtual asset, such as ETH, into a more stable one, such as USDT.

61. In total, 0x9AF, over its lifespan, received approximately 9,827,038.58 USDT. Of that, the majority of the USDT 0x9AF received, about 5,034,005.88 USDT (about 51.2%), was done as a result of the ETH to USDT swaps conducted by 0x9AF via Tokenlon. The second largest supplier of USDT to 0x9AF is a different unhosted address, 0x86d63D835B0ff15D5719D4D155F2A169fE692a42 (0x86), which sent approximately 2,832,044.75 USDT to 0x9AF, representing about 28.8% of the total USDT received by 0x9AF.

62. Under the circumstances, 0x86 is likely a separate consolidation wallet within the greater investment fraud scheme. Over its lifespan, 0x86 received a total of approximately 2,9251,54.16 USDT. Of that, at least 923,432.95 USDT came either directly or indirectly from other clusters identified associated with scams. These scams include, but are not limited to, NASDAWEB.com, NASDAQALL.com, and NASMOT.com.

63. Ultimately, the FBI obtained a lawful seizure warrant for the contents of 0x9AF on August 23, 2024. The seizure warrant was served on Tether on August 27, 2024.

64. On or about August 28, 2024, 0x9AF received one additional deposit of 30,000 USDT, bringing the total balance to 330,000.026094 USDT. It is this sum which is the Defendant Property.

65. Blockchain analysis conducted on this 30,000 USDT deposit showed a movement pattern similar to the victim's original losses. The funds originated from Crypto.com, were moved between 4 Ethereum addresses, one of which was a cluster associated with a different known scam website, EAG.cc, comingled with other funds, and eventually deposited into 0x9AF.

66. Based on my training and experience, there is probable cause to believe that the 0x9AF contains proceeds of violations of 18 U.S.C. § 1343 (wire fraud) and property involved in violations of 18 U.S.C. §§ 1956(a)(1)(B)(i) and 1957. Specifically, as the Defendant Property is involved in money laundering it is subject to forfeiture.

**CLAIM FOR RELIEF**  
**(Forfeiture under 18 U.S.C. § 981(a)(1)(A))**

67. The United States incorporates by reference paragraphs 1 – 66 above as if fully set forth herein.

68. Title 18, United States Code, Section 981(a)(1)(A) subjects to forfeiture “[a]ny property, real or personal, involved in a transaction or attempted transaction in violation of section 1956 . . . of this title, or any property traceable to such property.”

69. Title 18, United States Code, Section 1956(a)(1)(B)(i) imposes criminal liability on “[w]hoever, knowing that the property involved in a financial transaction represents the proceeds of some form of unlawful activity, conducts or attempts to conduct such a financial

transaction which in fact involves the proceeds of specified unlawful activity . . . knowing that the transaction is designed in whole or in part to conceal or disguise the nature, the location, the source, the ownership, or the control of the proceeds of specified unlawful activity.”

70. As set forth above, the Defendant Property constitutes property involved in a violation of section 1956.

71. As such, the Defendant Property is subject to forfeiture to the United States pursuant to 18 U.S.C. § 981(a)(1)(A).

### **PRAYER FOR RELIEF**

WHEREFORE, the United States prays that due process issue to enforce the forfeiture of the Defendant Property and that due notice be given to all interested parties to appear and show cause why said forfeiture of the Defendant Property should not be decreed, that the Defendant Property be condemned and forfeited to the United States to be disposed of according to law, and for such other and further relief as this Honorable Court may deem just and proper.

DATED this 28 day of March 2025.

Respectfully submitted,


ERIK S. SIEBERT  
UNITED STATES ATTORNEY

By: /s/Annie Zanobini  
Annie Zanobini  
Assistant United States Attorney  
California Bar No. 321324  
2100 Jamieson Avenue  
Alexandria, Virginia 22314  
Office Number: (703) 299-3903  
Facsimile Number: (703) 299-3982  
Email Address: [annie.zanobini2@usdoj.gov](mailto:annie.zanobini2@usdoj.gov)

VERIFICATION

I, Yanira Nieves, Special Agent with the Federal Bureau of Investigation, declare under penalty of perjury as provided by 28 U.S.C. § 1746, that the foregoing Complaint for Forfeiture in Rem is based on information known by me personally and/or furnished to me by various federal, state, and local law enforcement agencies, and that everything contained herein is true and correct to the best of my knowledge.

Executed at Mannassas, Virginia, this 28 of March, 2025

  
\_\_\_\_\_  
Yanira Nieves, Special Agent  
Federal Bureau of Investigation